Exhibit F

RIDGEVIEW MEDICAL CENTER AND CLINICS #3503

SUBJECT: ADMINISTRATOR/SPECIAL ACCESS POLICY

ORIGINATING DEPT: MIS **DISTRIBUTION DEPTS:** All

ACCREDITATION/REGULATORY STANDARDS:

Original Date: 12/12 **Revision Dates:** **Reviewed Dates:**	**APPROVAL:** Administration: _____ Director: _____

PURPOSE:

The purpose of the Ridgeview Medical Center Account Management Policy is to establish the rules for the creation, monitoring, control, and removal of user accounts.

Audience

The Ridgeview Medical Center Account Management Policy applies equally to all individuals with authorized access to any Ridgeview Medical Center Information Resource.

POLICY:

- All accounts created must have an associated and documented request and approval.
- All users must sign the Ridgeview Medical Center Enterprise Information Security Governance Policy Acknowledgement before access is granted to an account or Ridgeview Medical Center Information Resources. (See Policy #3511 - *Enterprise Information Security Governance*)
- All accounts must be uniquely identifiable using the user name assigned by Ridgeview Medical Center IS.
- All default passwords for accounts must be constructed in accordance with the Ridgeview Medical Center Password Policy.
- All accounts must have a password expiration that complies with the Ridgeview Medical Center Password Policy, wherever possible.
- Accounts used by individuals on extended leave (more than 30 days) will be disabled.
- All new user accounts that have not been accessed within 30 days of creation will be disabled.
- System Administrators, or other designated personnel:
  - Are responsible for modifying and/or removing the accounts of individuals that change roles with Ridgeview Medical Center or are separated from their relationship with Ridgeview Medical Center.
  - Must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes, and permission changes.
  - Must have a documented process for periodically reviewing existing accounts for validity
  - Are subject to independent audit review.
  - Must provide a list of accounts for the systems they administer when requested by authorized Ridgeview Medical Center IS Management personnel.
  - Must cooperate with authorized Ridgeview Medical Center Information Security personnel investigating security incidents at the direction of Ridgeview Medical Center Executive Management.

WAIVERS:

Waivers from certain policy provisions may be sought following the process outlined in the Ridgeview Medical Center Policy #3511 - *Enterprise Information Security Governance*.

ENFORCEMENT:

Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights and termination of contract(s).

VERSION HISTORY OF SOURCE DOCUMENT: Ridgeview Medical Center Information Security Policy Manual

Version Number	Date	Reason/Comments
V1.00	December, 2012	Document Origination
V2.00	May, 2014	Full review with IT Steering Committee
V3.00	August, 2015	Reviewed with Security Committee
	6/16	Finalized, assigned policy number, on RidgeNet. Previous documentation not archived.